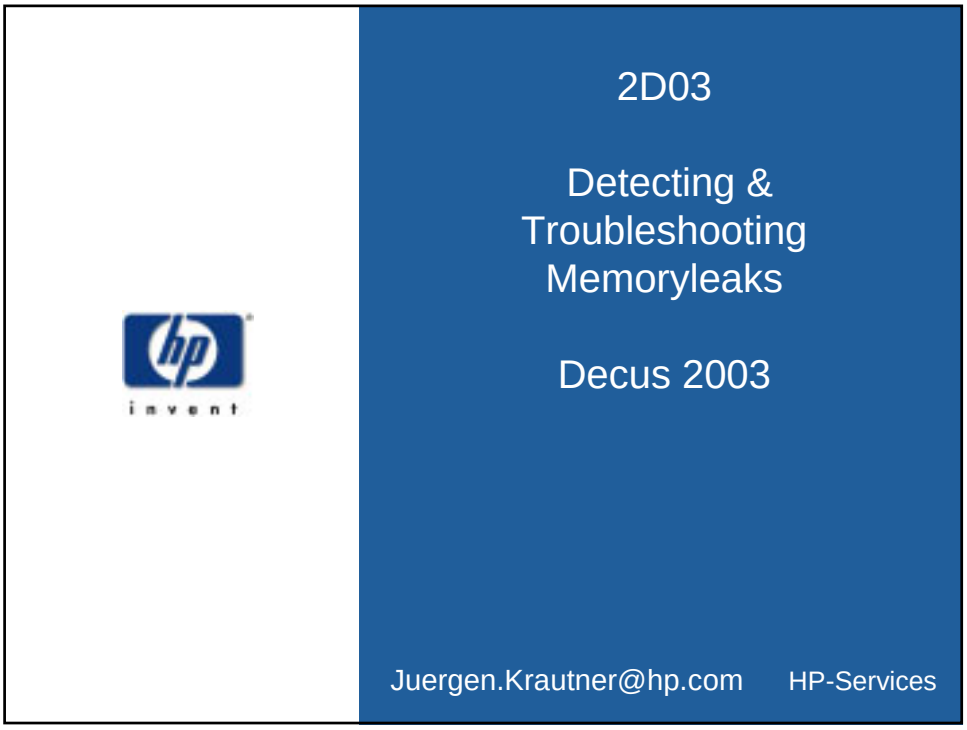


Agenda

- Memory Management
- Arten von Memory leaks
  - User mode
  - Kernel Modes
- Troubleshooting Tools
  - Applikation
  - Services
  - Drivers
- Demos

Hintergrund / Supporterfahrungen

- System “hängt”
  - Mouse, Capslock
  - Logon
  - Server Service (Events)
- schlechte Responsezeiten
- ABER: „ping“ geht immer
  - kernelmode stack

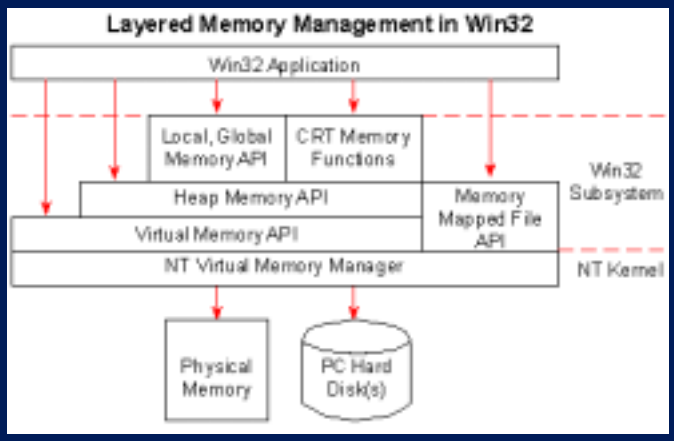
- Problem
  - **Zu spät ! Seien Sie vorbereitet. Es passiert wieder ..**

Leaks sind eine Plage.

- Windows 2000
  - mehr als 400 Leaks „geschlossen“
- Dutzende KB-Artikel
  - Server Service
  - RPC service
  - RAS
  - Performance Monitor
  - LMRepl
  - ASP …
- Backup-Software, Virenscanner etc

Memory Management

- Heap
- Paged Pool
- NonPaged Pool



Q126402 - PagedPoolSize and NonPagedPoolSize Values in Windows NT

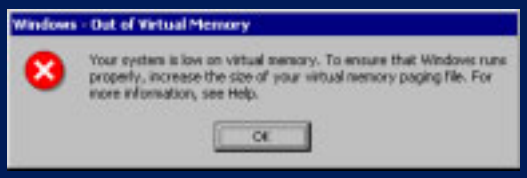
Wie entstehen Memory Leaks ...

- Resource Allocation ohne zugehöriges Release
  - von Heap, Virtual memory, Handles, Semaphore, Mutexes, …
- Thread Creation ohne Delete
- Functions
  - new(), malloc(), GlobalAlloc(),HeapAlloc(), CoTaskMemAlloc(), CreateFileMapping(), ExAllocatePoolWithTag() u.v.m.

```
Bool PrepInfo() {
  char * pBuffer = new char[10240];
  char * pResult;
  n = CopyInfo(pBuffer,pResult);
   if ( n < 0 )
       return FALSE;  // MEMORY LEAK!
  delete[] pBuffer ;
return TRUE;
  // MEMORY LEAK
free pResult
}
```

Wie machen sich Leaks bemerkbar

- Usermode:
  - Performanceverlust
  - Phys.Mem und Pagefile voll
  - evtl Popups



- Kernel Mode:
  - Hänger bis wieder Resourcen frei werden (aber Free & Allocs im Wettstreit …)
  - Eventlog

"**The server was unable to allocate the nonpaged pool from the system because the pool was empty**"

Troubleshooting

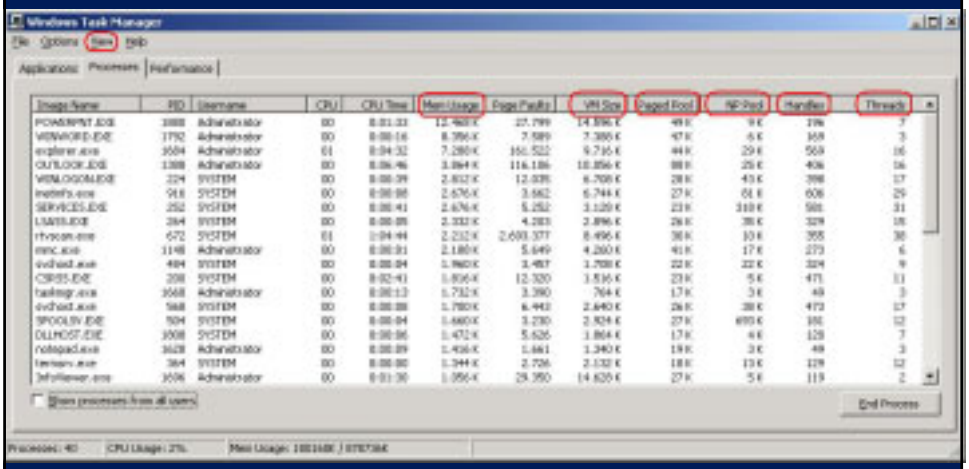
- Generelle Performance Problem ausschliessen
  - RAM, Disk I/O, CPU, Netzwerk
- BASELINE
  - Infos über das System im Normalzustand !
  - # Threads
  - Pagedpool-, Nonpaged Pool-, Pagefile-Usage
- Geduld, Geduld, Geduld

Tools
Identifizieren/Anzeigen

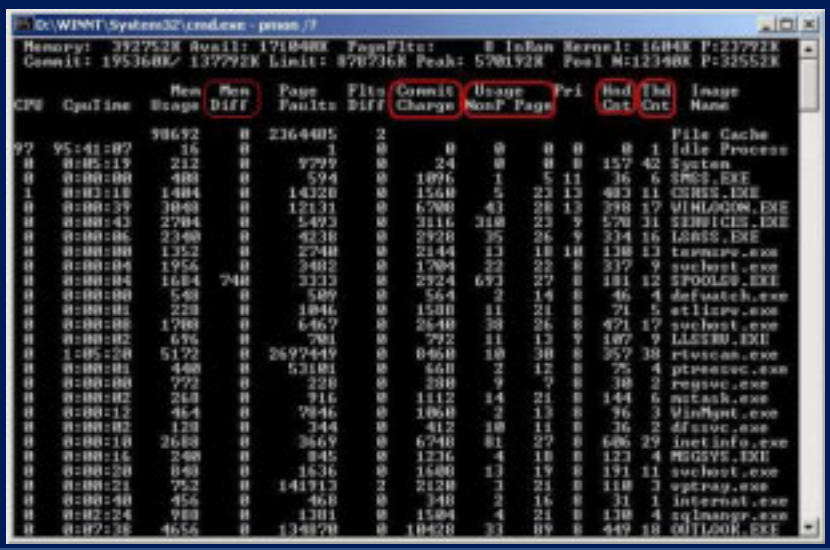
- Prozess Ids
- PagedPool Statistics
- NonPagedPool Statistics
- Pagefile Info
- Pool Tags
- Socket / Port Infos
- Treiberinfo

Applikationen
&
Services

Tools: Taskman



Tools: PMon



Tools: memsnap

```
C:\Type memsnap.log
Process ID         Proc.Name Wrkng.Set PagedPool  NonPgdPl  Pagefile    Commit   Handles   Threads
00000000             (null)     16384         0         0         0         0         0         1
00000008             System    229376         0         0     24576     24576       196        41
000000AC           SMSS.EXE    327680      4968      1200    147456    147456        36         6
000000C8           CSRSS.EXE   1085440     43644      6560   1413120   1413120       490        11
000000E0        WINLOGON.EXE   2002944     37244     55664   5959680   5959680       399        17
000000FC        SERVICES.EXE   6205440     30948    336804   2805760   2805760       570        32
00000108           LSASS.EXE   5955584     30460     37144   2756608   2756608       338        17
00000168         termsrv.exe   3854336     22304     14120   2023424   2023424       127        12
000001DC         svchost.exe   3817472     28244     24840   1544192   1544192       305         9
000001F0         SPOOLSV.EXE   4395008     30224    710412   2813952   2813952       166        12
0000020C        defwatch.exe   1826816     16032      2188    507904    507904        46         4
0000021C         svchost.exe   5902336     34724     42656   2281472   2281472       347        17
0000023C          LLSSRV.EXE   2179072     16384     12396    745472    745472       108         9
00000258         rtvscan.exe  10829824     37612     11668   8425472   8425472       358        38
000002B8          regsvc.exe    790528      8064      9548    245760    245760        30         2
000002D0          mstask.exe   3141632     25592     15724   1028096   1028096       144         6
00000380         WinMgmt.exe    450560     35588     17316   3158016   3158016       310         5
00000380          dfssvc.exe   1269760     12344     10588    385024    385024        36         2
```

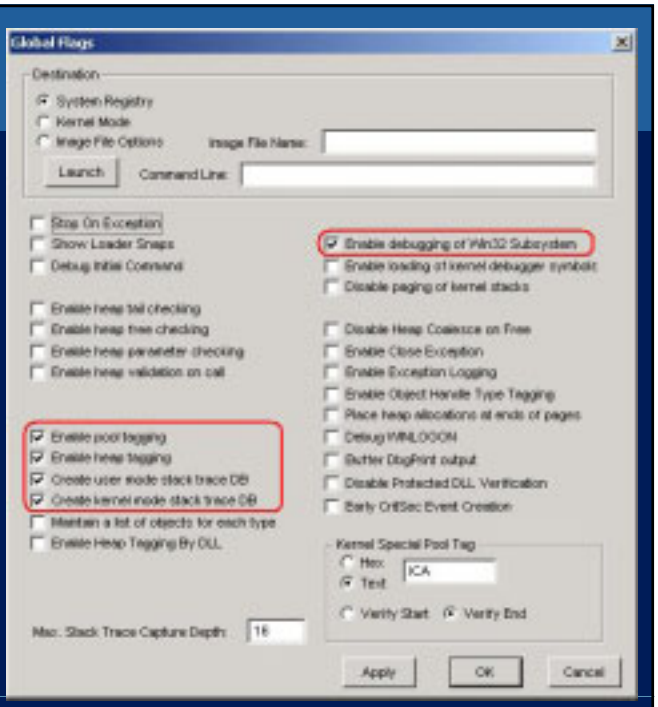

Tools: Tlist –s (-t)

```
D:\ tlist -s
   0 System Process
   8 System
 172 SMSS.EXE
 200 CSRSS.EXE       Title:
 224 WINLOGON.EXE    Title: NetDDE Agent
 252 SERVICES.EXE    Svcs:  Alerter,Browser,Dhcp,dmserver,Dnscache,Eventlog,
                            lanmanserver,lanmanworkstation,LmHosts,Messenger,
                            PlugPlay,ProtectedStorage,seclogon,TrkWks,Wmi
 264 LSASS.EXE       Svcs:  PolicyAgent,SamSs
 364 termsrv.exe     Svcs:  TermService
 484 svchost.exe     Svcs:  RpcSs
 552 etlisrv.exe     Svcs:  ELIService
 568 svchost.exe     Svcs:  EventSystem,Netman,NtmsSvc,RasMan,SENS
 672 rtvscan.exe     Svcs:  Norton AntiVirus Server
1684 explorer.exe    Title: Program Manager
1168 notepad.exe     Title: decusideas.txt - Notepad
1784 notepad.exe     Title: leaky cluster.txt - Notepad
1792 WINWORD.EXE     Title: mem.rtf - Microsoft Word
1628 notepad.exe     Title: vortrag.txt – Notepad
1668 taskmgr.exe     Title: Windows Task Manager
1060 inetinfo.exe    Svcs:  IISADMIN,MSFTPSVC,SMTPSVC,W3SVC
...
```

Tools: Gflags.exe

- -r =boot settings
- -k = kernel(current)
- -i =image

erfordert Reboot !



Tools: VaDump

- vadump -o -p 1668 vadump –s …

```
...
                                 Total        Private  Shareable    Shared
                               Pages    KBytes    KBytes    KBytes    KBytes
      Page Table Pages            18        72        72         0         0
      Other System                 3        12        12         0         0
      Code/StaticData             64       256        48         0       208
      Heap                        16        64        64         0         0
      Stack                        1         4         4         0         0
      Teb                          1         4         4         0         0
      Mapped Data                 21        84         0         0        84
      Other Data                   6        24        20         4         0

      Total Modules               64       256        48         0       208
      Total Dynamic Data          45       180        92         4        84
      Total System                21        84        84         0         0
Grand Total Working Set          130       520       224         4       292

Module Working Set Contributions in pages
    Total   Private Shareable    Shared Module
        3         2         0         1 NOTEPAD.EXE
       12         2         0        10 ntdll.dll
        8         1         0         7 GDI32.dll
        7         2         0         5 KERNEL32.DLL
```

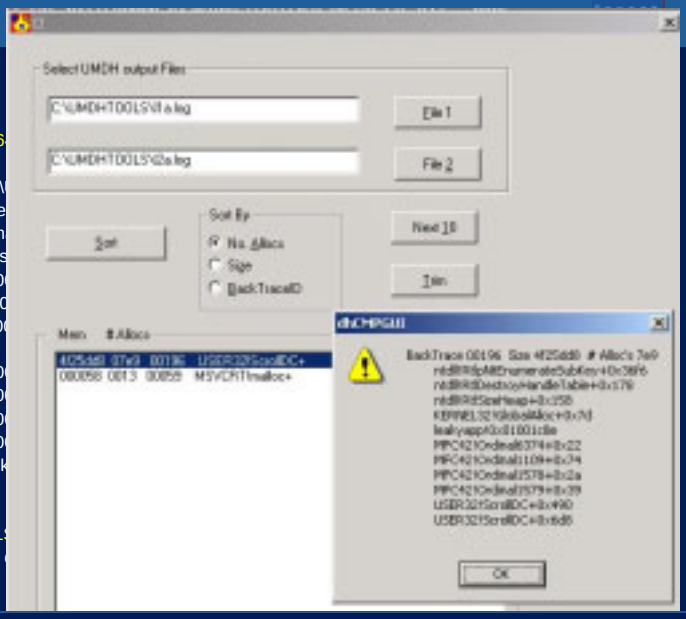
Tools: VaDump

- Monitor modus
- vadump -w -p 1576 (z.b. leakyapp)

```
. . .
  23107, RtlFillMemoryUlong+10
   2302, RtlSizeHeap+5c9
      7, RtlSizeHeap+e03
      4, DefWindowProcW+c6
      4, SetBkColor+38
      2, memmove+db
      2, SelectObject+4a
      2, RtlAllocateHeap+35
      2, CallNextHookEx+7b
      1, RtlGetCallersAddress+2d8
      1, RtlGetCallersAddress+137
...
```

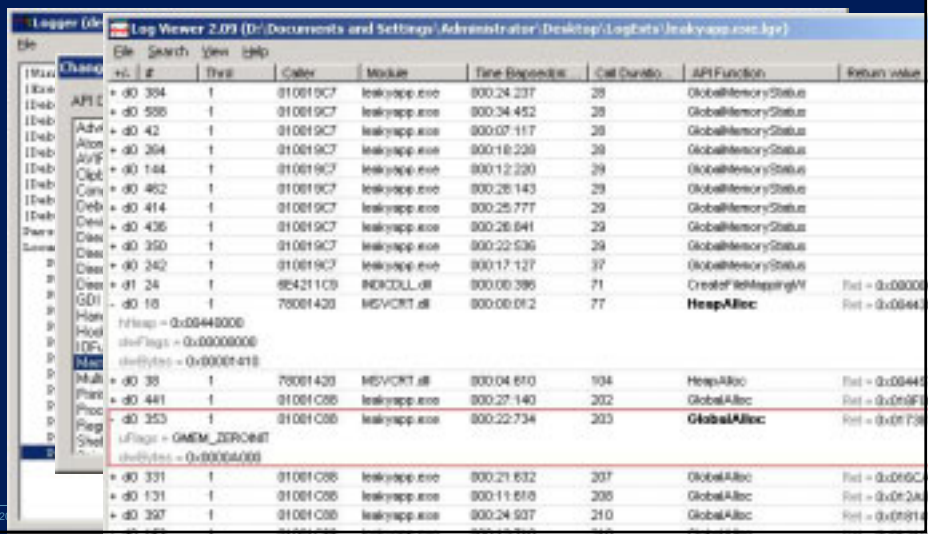

Tools: dh, dhcmp, dhcmpgui

1) leakyapp
2) Tlist (für Prozess ID)
3) C:\UMDHTOOLS> dh -p 66
SetThreadPriority failed: 6
DH: Writing dump output to C:\
RtlCreateQueryDebugBuffer re
RtpQueryProcessDebugInform
  ProcessId: 664 ProcessFlags
Loading symbols for 0x010000
Loading symbols for 0x77f800
Loading symbols for 0x6c3700
...
Loading symbols for 0x77d400
Loading symbols for 0x6e4200
Loading symbols for 0x75e600
Loading symbols for 0x060500
Getting symbols for Stack Back
C:\UMDHTOOLS>
 .. start leaking ...
4) dh -p 664 -f C:\UMDHTOOL
5) dhcmpgui ... sort by size ...



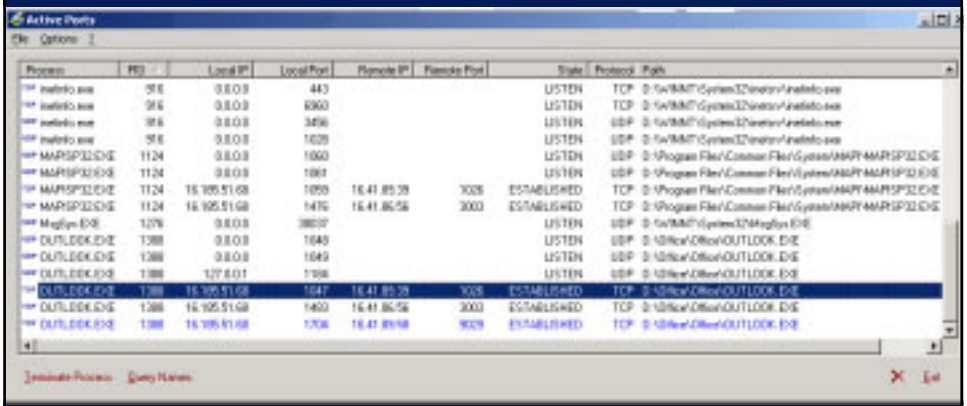
Tools: Logger & Logviewer

- logger "D:\Program Files\Resource Kit\leakapp.exe



Tools: netstat –a (bzw. ActivePort)

```
Active Connections
```

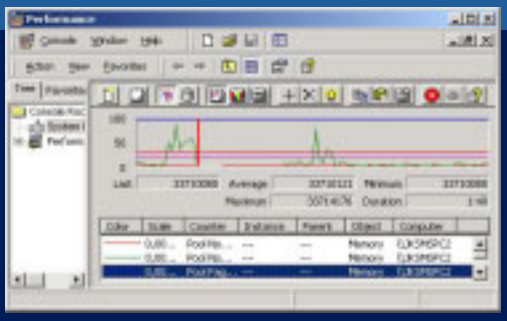


- ActivePort: http://www.ntutility.com/freeware.html
- .net: netstat –o (owner)

Treiber

Tools: Perfmon

- Paging File
  - % Usage, %Usage Peak
- Memory
  - Pool Nonpaged Bytes, Pool Paged Bytes
- Process
  - Page File Bytes,
  - Pool Nonpaged Bytes, Pool Paged Bytes,
  - Private Bytes, Thread Count



- ALERTS / LOGS
  - Counter
  - Script / send Msg

How to Create a Performance Monitor Log for NT Troubleshooting [Q150934]

How to Monitor a Remote Computer Without Logging On to It [Q246758]

Tools: Drivers.exe

```
C:\ drivers
  ModuleName    Code    Data     Bss   Paged    Init         LinkDate
-------------------------------------------------------------------------------
ntoskrnl.exe  442368   97216       0  775488  139264  Sat Apr 14 02:52:32 2001
     hal.dll   25952    6048       0   16544   10272  Wed Nov 29 05:34:07 2000
 BOOTVID.DLL    5664    2464       0       0     320  Thu Nov 04 02:24:33 1999
    ACPI.sys   92096    9024       0   43520    4448  Wed Oct 25 21:59:00 2000
  WMILIB.SYS     512       0       0    1152     192  Sat Sep 25 19:36:47 1999
     pci.sys   12864    1536       0   31456    4640  Fri Mar 02 01:38:34 2001
  isapnp.sys   14368     832       0   22944    2272  Mon Aug 28 06:40:00 2000
compbatt.sys    2496       0       0    2880    1216  Mon Aug 28 09:02:21 2000
   BATTC.SYS     800       0       0    3008     704  Mon Aug 28 09:02:18 2000
  pciide.sys     672      32       0       0     128  Mon Aug 28 06:39:25 2000
 PCIIDEX.SYS    4544     480       0   10944    1632  Mon Aug 28 06:39:25 2000
intelide.sys    1984      32       0       0     128  Mon Aug 28 06:39:24 2000
  pcmcia.sys   32960    8864       0   23904    6272  Wed Feb 07 03:17:01 2001
  ftdisk.sys    4640      32       0   95072    3392  Mon Nov 22 20:36:23 1999
Diskperf.sys    1728      32       0    2016    1088  Fri Oct 01 01:30:40 1999
    dmio.sys  105568   15168       0       0    2752  Mon Aug 28 06:42:30 2000
 PartMgr.sys     576       0       0    6656    1376  Fri Oct 15 01:59:16
…
```

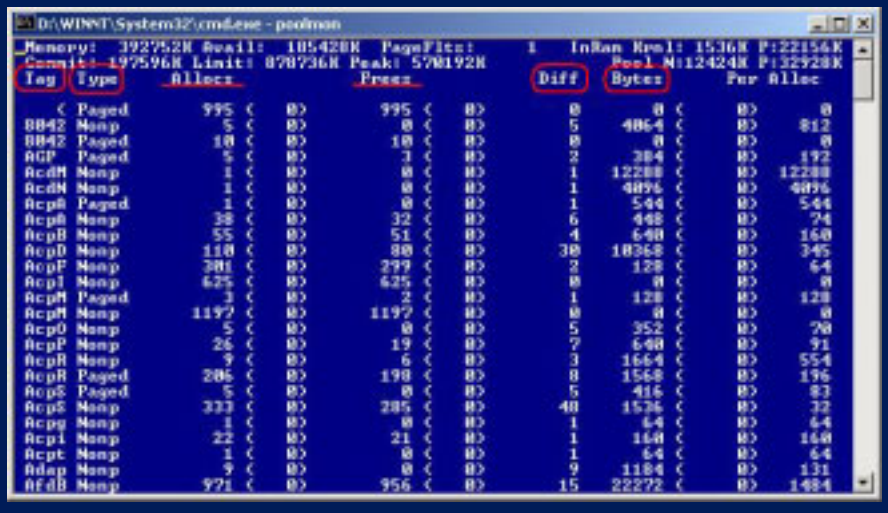

Tools: pstat

```
C:\ PSTAT

 Memory: 392752K Avail: 197908K  TotalWs: 173552K InRam Kernel: 1644K P:24336K
 Commit: 193156K/ 135804K Limit: 878736K Peak: 570192K  Pool N:12232K P:32344K
    User Time   Kernel Time    Ws    Faults  Commit Pri Hnd Thd Pid Name
                             90832  2414658                          File Cache
  0:00:00.000   1:49:10.687    16        1       0  0    0   1   0 Idle Process
  0:00:00.000   0:05:37.635   212    10006      24  8  160  42   8 System
  0:00:00.010   0:00:00.821   408      594    1096 11   36   6 172 SMSS.EXE
  0:00:41.669   0:03:15.641  1632    17587    1532 13  464  11 200 CSRSS.EXE
..
ModuleName Load Addr     Code    Data    Paged          LinkDate
-------------------------------------------------------------------------------
ntoskrnl.exe 804D2000  442368   97216  775488 Sat Apr 14 03:52:32 2001
     hal.dll 80675000   25952    6048   16544 Wed Nov 29 05:34:07 2000
 BOOTVID.DLL EC410000    5664    2464       0 Thu Nov 04 02:24:33 1999
    ACPI.sys BFFD8000   92096    9024   43520 Wed Oct 25 22:59:00 2000
  WMILIB.SYS EC5C8000     512       0    1152 Sat Sep 25 20:36:47 1999
     pci.sys EC000000   12864    1536   31456 Fri Mar 02 01:38:34 2001
```

Tools: perfmtr.exe

```
CPU Usage  Page Page Page InCore NonP Pgd  Incore Pgd  Incore Incore Proc Thd
           Flts Aval Pool PgPool Pool Krnl  Krnl  Drvr  Drvr  Cache  Cnt  Cnt
*         |  87 54852 8085 (6078) 3058  193 (  98)  640 ( 313) (14545)  51  402
*         |   3 54844 8085 (6078) 3058  193 (  98)  640 ( 313) (14545)  51  402
*         |   4 54863 8085 (6078) 3058  193 (  98)  640 ( 313) (14545)  51  402

Server
  Bytes    Bytes     Paged NonPaged                Logn Witm
  Rcvd     Sent      Pool      Pool Sess File Srch Errs Shtg
     0        0     11549   2444323    1    0    0    0    0
     0        0     11549   2444323    1    0    0    0    0
Pool
Paged Paged Paged  Non    Non    Non     Page Paged Non    Commit  Commit SysPte
Alloc Freed   A-F  Alloc Freed  A-F     Aval Pages Pages  Pages   Limit   Free
   21    70 40549    28    28 36030     7154  7808  2338  43997 120725   43064
   24    36 40537    22    22 36030     7156  7808  2338  43997 120725   43064
 1213  1630 40120   156   142 36044     7348  7829  2349  44028 120725   43064
   10    10 40120    34    35 36043     7339  7829  2349  44028 120725   43064
I/O
 Read Write Other      Read     Write     Other      File       File
 I/Os  I/Os  I/Os      Xfer      Xfer      Xfer     Objects    Handles
    2     0    24        24         0         0         0         44
    7     6    34       364         0       316         0        360
```


Tools: Poolmon.exe

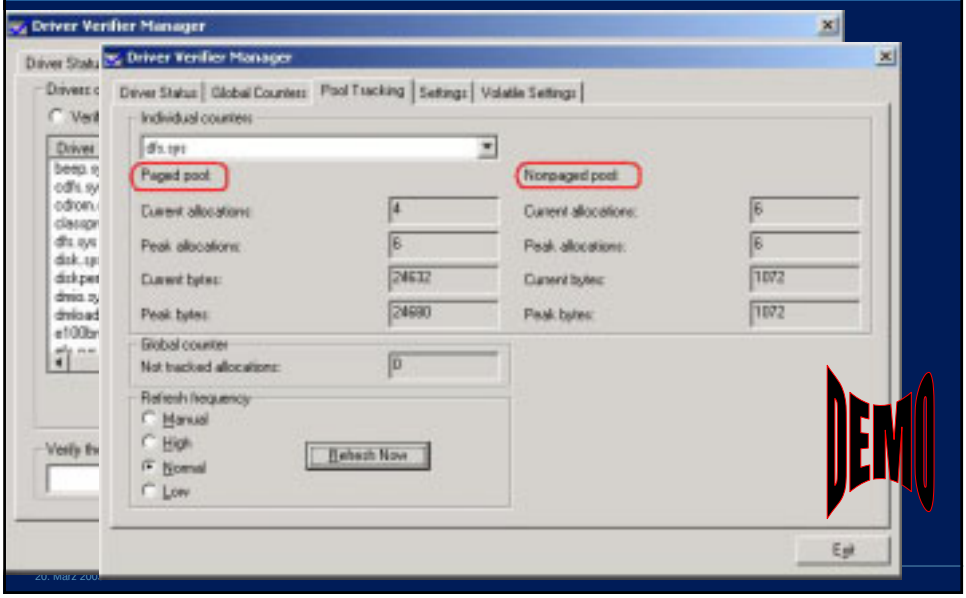


q=quit, p=pooltoggle, f=free, t=tag, b=bytes, a=alloc, l=highlight, m=per alloc

Tools: Poolmon Infos ...

- Q177415
  How to Use Poolmon to Troubleshoot Kernel Mode Memory Leaks
- Q164933
  How to Allow Poolmon.exe to Run by Setting GlobalFlag Value
- Tag-Liste ?
  - …\Debugging Tools for Windows\triage\pooltag.txt
    ...
    Dfb - framebuf video driver
    Dfs - Distributed File System
    Djz - jzvxl484 video driver
    Dlck - deadlock verifier (part of driver verifier) structures
    Dmio - Logical Disk Manager driver
    DPrf - Disk performance filter driver - diskperf.c
    ...
  - findstr /m "IpAT" *.sys (→..\drivers\ipsec.sys)

Tools: Driver Verifier (verifier.exe)



Workarounds

- Temporäre Lösung:
  - Pagefile vergrößern
  - Regelmäßiger Reboot
  - Restart von Applikation
  - Restart von Services (at, net stop…)
- Wenn möglich:
  - Treiberupdate
  - Applikation Hotfix/Update
  - OS-Hotfix / Servicepack
  - 64 bit ;-)
- Crashdump Auswertung "CrashOnCtrlScroll"
  - Q244139 Windows Feature Allows a Memory.dmp File to Be Generated

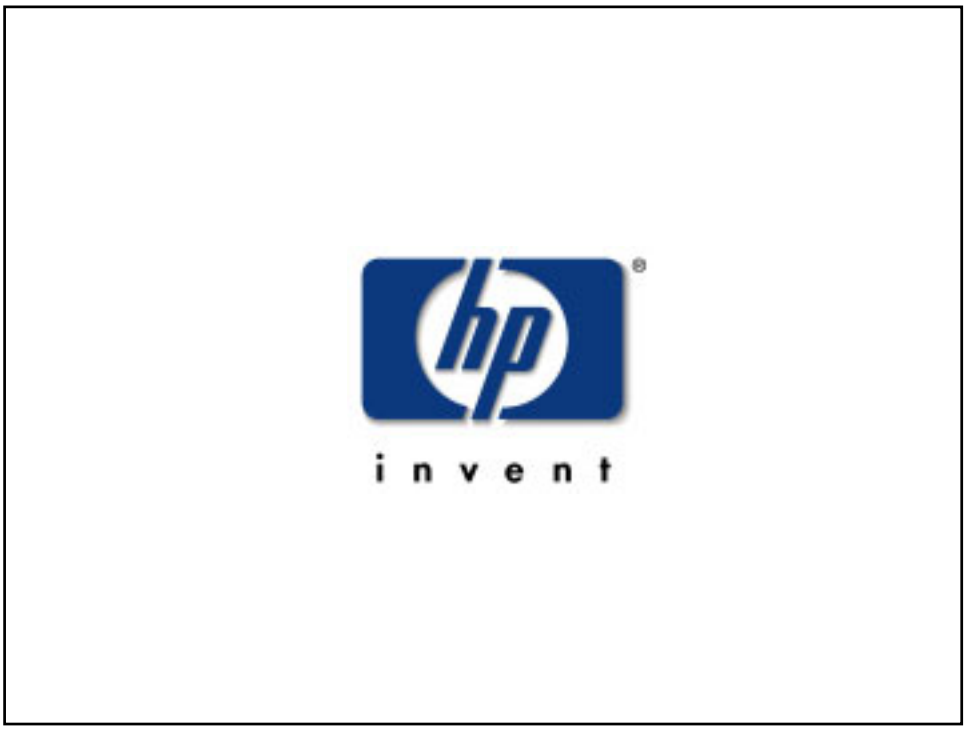
KB-Artikel

- Q150934 How to Create a Performance Monitor Log for NT Troubleshooting
- Q177415 How to Use Poolmon to Troubleshoot Kernel Mode Memory Leaks
- Q286350 HOWTO: Use Autodump+ to Troubleshoot "Hangs" and "Crashes"
- Q251233 Considerations When Using Driver Verifier on Production Servers
- Q268343 Umdhtools.exe: How to Use Umdh.exe to Find Memory Leaks
- Q192486 INFO: Introduction to Windows NT Kernel Special Pool
- Q126402 PagedPoolSize and NonPagedPoolSize Values in Windows NT
- Q229902 Driver Verifier Always Performs Certain Kernel-Mode Driver Tests
- Q229903 Partial List of Possible Error Codes with Driver Verifier
- Q244617 Using Driver Verifier to Troubleshoot Drivers in Win 2K and XP
- Q243318 How to Use Dh.exe to Troubleshoot User-Mode Memory Leaks
- Q290620 HOWTO: Create an Alert to Automatically Generate a Dump Heap Log
- Q253706 HOWTO: Isolate and Identify the Source of Inetinfo or Other Process Memory Leaks"
- Q286568 Use Application Verifier to Troubleshoot Programs in Windows XP
- w2k reskit : Chapter 6 - Evaluating Memory and Cache Usage
  - Investigating memory shortages => perfmon counters screenshots
  - Investigating disk paging
  - Investigating user-mode memory leaks
  - Investigating kernel-mode memory leaks
  - Monitoring the cache
  - Resolving memory and cache bottlenecks

Tools

- Windows 2000 Resourcekit
  - http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp
- W2000 Support Tools (2000RKST.MSI)
  - W2000 Server CD (Support)
- Debugging Tools for Windows
  - http://www.microsoft.com/ddk/debugging/installx86beta.asp
- OEM Support Tools Phase 3 Release Notes
  - http://download.microsoft.com/download/win2000srv/Utility/3.0/NT45/EN-US/Oem3sr2.zip
- UMDH-Tools
  - http://download.microsoft.com/download/win2000platform/utility/1/NT5/EN-US/umdhtools.exe

Fragen ?


invent